ADHOC NETWORKS

Dinesh Choudhary[1]**,Vijay Kumar**[2] **and Jyoti**[3]
[1]Department of Computer Science Engineering, KITE, Jaipur, Rajasthan Technical University, Kota, Dinesh_matwa@yahoo.co.in
[2]Department of Computer Science Engineering, SMCET, Jaipur, Rajasthan Technical University, Kota, Vijay_matwa@yahoo.com
[3]Department of ECE, SMCET, Jaipur, Rajasthan Technical University, Kota, Jyoti_matwa@yahoo.in

Abstract- Ad hoc networks are a new wireless networking paradigm for mobile hosts. Unlike traditional mobile wireless networks, ad hoc networks do not rely on any fixed infrastructure. Instead, hosts rely on each other to keep the network connected. The military tactical and other security-sensitive operations are still the main applications of ad hoc networks, although there is a trend to adopt ad hoc networks for commercial uses due to their unique properties. One main challenge in design of these networks is their vulnerability to security attacks. In this paper, we study the threats an ad hoc network faces and the security goals to be achieved. We identify the new challenges and opportunities posed by this new networking environment and explore new approaches to secure its communication. In particular, we take advantage of the inherent redundancy in ad hoc networks multiple routes between nodes to defend routing against denial of service attacks. We also use replication and new cryptographic schemes, such as threshold cryptography, to build a highly secure and highly available key management service, which forms the core of our security framework.

Ad hoc is a Latin phrase which means "for this [purpose]". It generally signifies a solution designed for a specific problem or task, non-generalisable and which cannot be adapted to other purposes. Common examples are organizations, committees and commissions created at the national or international level for a specific task; in other fields the term may refer, for example, to a tailor-made suit, a handcrafted network protocol or a purpose-specific equation. Ad hoc can also have connotations of a makeshift solution, inadequate planning or improvised events. Other derivates of the Latin include AdHoc, adhoc and ad-hoc.

1. Introduction

Ad hoc networks are a new paradigm of wireless communication for mobile hosts (which we call nodes). In an ad hoc network, there is no fixed infrastructure such as base stations or mobile switching centers. Mobile nodes that are within each other's radio range communicate directly via wireless links, while those that are far apart rely on other nodes to relay messages as routers. Node mobility in an ad ho c network causes frequent changes of the network topology. Military tactical operations are still the main application of ad hoc networks today. For example, military units (e.g., soldiers, tanks, or planes), equipped with wireless communication devices, could form an ad ho c network when they roam in a battlefield. Ad hoc networks can also be used for emergency, law enforcement, and rescue missions. Since an ad hoc network can be deployed rapidly with relatively low cost, it becomes an attractive option for commercial uses such as sensor networks or virtual classrooms.

1.1 Security Goals

Security is an important issue for ad hoc networks, especially for those security-sensitive applications. To secure an ad hoc network, we consider the following attributes: availability, confidentiality, integrity, authentication, and non-repudiation. Availability ensures the survivability of network services despite denial of service attacks. A denial of service attack could be launched at any layer of an ad ho c network. On the physical and media access control layers, an adversary could employ jamming to interfere with communication on physical channels. On the network layer, an adversary could disrupt the routing protocol and disconnect the network. On the higher layers, an adversary could bring down high-level services. One such target is the key management service, an essential service for any security framework. Confidentiality ensures that certain information is never disclosed to unauthorized entities. Network transmission of sensitive information, such as strategic or tactical military information, requires confidentiality. Leakage of such information to enemies could have devastating consequences. Routing information must also remain confidential in certain cases, because the information might be valuable for enemies to identify and to locate their targets in a battlefield.

Integrity guarantees that a message being transferred is never corrupted. A message could be corrupted because of benign failures, such as radio propagation impairment, or because of malicious attacks on the network.

Authentication enables a node to ensure the identity of the peer node it is communicating with. Without authentication, an adversary could masquerade a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of other nodes. Finally, non-repudiation ensures that the origin of a message cannot deny having sent the message. Non- repudiation is useful for detection and isolation of compromised nodes. When a node A receives an erroneous message from a node B, non-repudiation allows A to accuse B using this message and to convince other nodes that B is compromised. There are other security goals (e.g., authorization) that are of concern to certain applications, but we will not pursue these issues in this paper.

1.2 Challenges

The salient features of ad hoc networks pose both challenges and opportunities in achieving these security goals. First, use of wireless links renders an ad hoc network susceptible to link attacks ranging from passive eavesdropping to active impersonation, message replay, and message distortion. Eavesdropping might give an adversary access to secret information, violating confidentiality. Active attacks might allow the adversary to delete messages, to inject erroneous messages, to modify messages, and to impersonate a node, thus violating availability, integrity, authentication, and non-repudiation. Secondly, nodes, roaming in a hostile environment (e.g., a battlefield) with relatively poor physical protection, have non-negligible probability of being compromised. Therefore, we should not only consider malicious attacks from outside a network, but also take into account the attacks launched from within the network by compromised nodes. Therefore, to achieve high survivability, ad hoc networks should have a distributed architecture with no central entities. Introducing any central entity into our security solution could lead to significant vulnerability; that is, if this centralized entity is compromised, then the entire network is subverted.

Thirdly, an ad hoc network is dynamic because of frequent changes in both its topology and its membership (i.e., nodes frequently join and leave the network). Trust relationship among nodes also changes, for example, when certain nodes are detected as being compromised. Unlike other wireless mobile networks, such as mobile IP nodes in an ad hoc network may dynamically become affiliated with administrative domains. Any security solution with a static configuration would not suffice. It is desirable for our security mechanisms to adapt on-the-fly to these changes. Finally, an ad hoc network may consist of hundreds or even thousands of nodes. Security mechanisms should be scalable to handle such a large network.

1.3 Scope and Roadmap

Traditional security mechanisms, such as authentication protocols, digital signature, and encryption, still play important roles in achieving confidentiality, integrity, authentication, and non-repudiation of communication in ad hoc networks. However, these mechanisms are not sufficient by themselves.We further rely on the following two principles. First, we take advantage of redundancies in the network topology (i.e., multiple routes between nodes) to achieve availability. The second principle is distribution of trust. Although no single node is trustworthy in an ad hoc network because of low physical security and availability, we can distribute trust to an aggregation of nodes. Assuming that any t + 1 nodes will unlikely be all compromised, consensus of at least t + 1 nodes is trustworthy. All key-based cryptographic schemes (e.g., digital signature) demand a key management service, which is responsible for keeping track of bindings between keys and nodes and for assisting the establishment of mutual trust and secure communication between nodes.

2. Secure Routing

To achieve availability, routing protocols should be robust against both dynamically changing topology and malicious attacks. Routing protocols proposed for ad hoc networks cope well with the dynamically changing topology. However, none of them, to our knowledge, have accommodated mechanisms to defend against malicious attacks. Routing protocols for ad hoc networks are still under active research. There is no single standard routing protocol. Therefore, we aim to capture the common security threats and to provide guidelines to secure routing protocols.

In most routing protocols, routers exchange information on the topology of the network in order to establish routes between nodes. Such information could become a target for malicious adversaries who intend to bring the network down. There are two sources of threats to routing protocols. The first comes from external attackers. By injecting erroneous routing information, replaying old routing information, or distorting routing information, an attacker could successfully partition a network or introduce excessive traffic load into the network by causing retransmission and inefficient routing. The second and also the more severe kind of threats comes from compromised nodes, which might advertise incorrect routing information to other nodes. Detection of such incorrect information is difficult: merely requiring routing information to be signed by each node would not work, because compromised nodes are able to generate valid signatures using their private keys.

To defend against the first kind of threats, nodes can protect routing information in the same way they protect data traffic, i.e., through the use of cryptographic schemes such as digital signature. However, this defense is ineffective against attacks from compromised servers. Worse yet, as we have argued, we cannot neglect the possibility of nodes being compromised in an ad hoc network. Detection of compromised nodes through routing information is also difficult in an ad hoc network because of its dynamically changing topology: when a piece of routing information is found invalid, the information could be generated by a compromised node, or, it could have become invalid as a result of topology changes. It is difficult to distinguish between the two cases. On the other hand, we can exploit certain properties of ad hoc networks to achieve secure routing. Note that routing protocols for ad hoc networks must handle outdated routing information to accommodate the dynamically changing topology. False routing information generated by compromised nodes could, to some extent, be considered outdated information. As long as there are sufficiently many correct nodes, the routing protocol should be able to find routes that go around these compromised nodes. Such capability of the routing protocols usually relies on the inherent redundancies — multiple, possibly disjoint, routes between nodes — in ad hoc networks. If routing protocols can discover multiple routes (e.g., protocols in ZRP [16], DSR [25], TORA [32], and AODV [35] all can achieve this), nodes can switch to an alternative route when the primary route appears to have failed. Diversity coding takes advantage of multiple paths in an efficient way without message retransmission. The basic idea is to transmit redundant information through additional routes for error detection and correction. For example, if there are n disjoint routes between two nodes, then we can use n - r channels to transmit data and use the other r channels to transmit redundant information. Even if certain routes are compromised, the receiver may still be able to validate messages and to recover messages from errors using the redundant information from the additional r channels.

3. Key Management Service

We employ cryptographic schemes, such as digital signatures, to protect both routing information and data traffic. Use of such schemes usually requires a key management service.

We adopt a public key infrastructure because of its superiority in distributing keys and in achieving integrity and non-repudiation. Efficient secret key schemes are used to secure further communication after nodes authenticate each other and establish a shared secret session key. In a public key infrastructure, each node has a public/private key pair. Public keys can be distributed to other nodes, while private keys should be kept confidential to individual nodes. There is a trusted entity called Certification Authority (CA) for key management. The CA has a public/private key pair, with its public key known to every node, and signs certificates binding public keys to nodes. The trusted CA has to stay on-line to reflect the current bindings, because the bindings could change over time: a public key should be revoked if the owner node is no longer trusted or is out of the network; a node may refresh its key pair periodically to reduce the chance of a successful brute-force attack on its private key.

It is problematic to establish a key management service using a single CA in ad hoc networks. The CA, responsible for the security of the entire network, is a vulnerable point of the network: if the CA is unavailable, nodes cannot get the current public keys of other nodes or to establish secure communication with others. If the CA is compromised and leaks its private key to an adversary, the adversary can then sign any erroneous certificate using this private key to impersonate any node or to revoke any certificate. A standard approach to improve availability of a service is replication. But a naive replication of the CA makes the service more vulnerable: compromise of any single replica, which possesses the service private key, could lead to collapse of the entire system. To solve this problem, we distribute the trust to a set of nodes by letting these no des share the key management responsibility.

3.1 Asynchrony

Existing threshold cryptography and proactive threshold cryptography schemes assume a synchronous system (i.e., there is a bound on message-delivery and message-processing times). This assumption is not necessarily valid in an ad ho c network, considering the low reliability of wireless links and poor connectivity among nodes. In fact, any synchrony assumption is a vulnerability in the system: the adversary can launch denial of service attacks to slow down a node or to disconnect a node for a long enough period of time to invalidate the synchrony assumption. Consequently, protocols based on the synchrony assumption are inadequate.

To reduce such vulnerability, our key management service works in an asynchronous setting. Designing such protocols is hard; some problems may even be impossible to solve [8]. The main difficulty lies in the fact that, in an asynchronous system, we cannot distinguish a compromised server from a correct but slow one.

One basic idea underlying our design is the notion of weak consistency: we do not require that the correct servers be consistent after each operation; instead, we require enough correct servers to be up-to-date. For example, in share refreshing, without any synchrony assumption, a server is no longer able to distribute the subshares to all correct servers using a reliable broadcast channel. However, we only require subshares to be distributed to a quorum of servers. This suffices, as long as correct servers in such a quorum can jointly provide or compute all the subshares that are distributed. This way, correct servers not having certain subshare(s) could recover its subshare(s) from other correct servers.

Another important mechanism is the use of multiple signatures for correct servers to detect and to reject erroneous messages sent by compromised servers. That is, we require that certain messages be accompanied with enough signatures from servers. If a message contains digital signatures from a certain number (say, t + 1) of servers testifying its validity, at least one correct server must have provided one signature, thus establishing the validity of the message. We have implemented a prototype of such a key management service. The preliminary results have shown its feasibility. Due to the length restriction of this paper, we are unable to provide a detailed description of this service. Full papers describing the key management service and its underlying proactive secret sharing protocol in asynchronous system are in preparation.

4. Related Work

4.1 Secure Routing

Secure routing in networks such as the Internet has been extensively studied. Many proposed approaches are also applicable to secure routing in ad hoc networks. To deal with external attacks, standard schemes such as digital signatures to protect information authenticity and integrity have been considered. For example, Sirios and Kent propose the use of a keyed one-way hash function with windowed sequence number for data integrity in point-to-point communication and the use of digital signatures to protect messages sent to multiple destinations. Perlman studies how to protect routing information from compromised routers in the context of Byzantine robustness. The study analyzes the theoretical feasibility of maintaining network connectivity under such assumptions. Kumar recognizes the problem of compromised routers as a hard problem, but provides no solution. Other works give only partial solutions. The basic idea underlying these solutions is to detect inconsistency using redundant information and to isolate compromised routers. For example, in, where methods to secure distance-vector routing protocols are proposed, extra information of a predecessor in a path to a destination is added into each entry in the routing table. Using this piece of information, a path-traversal technique (by following the predecessor link) can be used to verify the correctness of a path. Such mechanisms usually come with a high cost and are avoided because routers on networks such as the Internet are usually well protected and rarely compromised.

4.2 Replicated Secure Services

The concept of distributing trust to a group of servers is investigated by Reiter. This is the foundation of the Rampart toolkit. Reiter and others have successfully used the toolkit in building a replicated key management service, which also employs threshold cryptography. One drawback of Rampart is that it may remove correct but slow servers from the group. Such removal renders the system at least temporarily more vulnerable. Membership changes are also expensive. For these reasons, Rampart is more suitable for tightly coupled networks than for ad ho c networks.

Gong applies trust distribution to Key Distribution Center (KDC), the central entity responsible for key management in a secret key infrastructure. In his solution, a group of servers jointly act as a KDC with each server sharing a unique secret key with each client. Malkhi and Reiter present Phalanx, a data repository service that tolerate Byzantine failures in an asynchronous system. The essence of Phalanx is a Byzantine quorum system. In a Byzantine quorum system, servers are grouped into quorums satisfying a certain intersection property. The service supports read and write operations and guarantees that a read operation always returns the result of the last completed write operation. Instead of requiring each correct server to perform each operation, the service performs each operation on only a quorum of servers. However, this weak consistency among the servers su ces to achieve the guarantee of the service because of the intersection property of Byzantine quorum systems.

Castro and Liskov extend the replicated state-machine approach to achieve Byzantine fault tolerance. They use a three-phase protocol to mask away disruptive behavior of compromised servers. A small portion of servers may be left behind, but can recover by communicating with other servers. None of the systems provide mechanisms to defeat mobile adversaries and to achieve scalable adaptability. The latter two solutions do not consider how a secret (a private key) is shared among the replicas. However, they are useful in building highly secure services in ad hoc networks. For example, we could use Byzantine quorum systems to secure a location database for an ad hoc network.

4.3 Security in Ad hoc Networks

In [22], an authentication architecture for mobile ad ho c networks is proposed. The proposed scheme details the formats of messages, together with proto cols that achieve authentication. The architecture can accommodate di erent authentication schemes. Our key management service is a prerequisite for such a security architecture.

5. Ad hoc committee, commission or organization

Ad hoc organizations, to include committees, are used when an objective needs consideration and no standing organ/committee within said organization can absorb that issue into its scope. Usually these committees are used on a temporary basis, such as temporary oversight of an issue, or review of the standing rules or the constitution of that organization.

An ad hoc organization may have, in some cases, a long term or indefinite duration of existence. In these cases, an initial workgroup or forum may give place to a more permanent form of organization. A typical example is the OSCE (Organization for Security and Co-operation in Europe).

6. Ad hoc hypothesis

In science and philosophy, ad hoc means the addition of extraneous hypotheses to a theory in order to save it from being falsified. Ad hoc hypotheses compensate for anomalies not anticipated by the theory in its unmodified form. Scientists are often skeptical of theories that rely on frequent, unsupported adjustments to sustain them. Ad hoc hypotheses are often characteristic of pseudoscientific subjects.[1] Much of scientific understanding relies on the modification of existing hypotheses or theories but these modifications are distinguished from ad hoc hypotheses in that the anomalies being explained propose a new means of being real.

Ad hoc hypotheses are not necessarily incorrect, however. An interesting example of an apparently supported ad hoc hypothesis was Albert Einstein's addition of the cosmological constant to general relativity in order to allow a static universe. Although he later referred to it as his "greatest blunder", it has been found to correspond quite well to the theories of dark energy [2].

7. Ad hoc pronunciation

Many reference works employ ad hoc pronunciation schemas as a way of indicating how words are pronounced. These are especially popular in U.S. published works, such as the Merriam-Webster dictionary. An example of an ad hoc pronunciation would be "DIK-shuh-nair-ee", where the capitalization shows which syllable is stressed. This is in contrast to systems such as the International Phonetic Alphabet, which attempt to put pronunciation schemes on a standard footing. Critics of ad hoc schemes point out that such schemes are inherently self-referential, since they rely on the ability of the reader to already know how a large number of words are commonly pronounced. As its name suggests, there is no "standard" ad hoc schema, and so examples will vary considerably according to the publication's whim. In contrast, the IPA seeks to base pronunciation solely on vocal tract configurations and on the phonemes produced, though very often neo-common simple words are used to illustrate how the IPA applies in a specific language. Proponents of ad hoc claim that it is much easier to use than IPA, though will often concur that this is usually only because the pronunciation is already known.

8. Ad hoc querying

Ad hoc querying is a term in information science. Many application software systems have an underlying database which can be accessed by only a limited number of queries and reports. Typically these are available via some sort of menu, and will have been carefully designed, pre-programmed and optimized for performance by expert programmers. By contrast, "ad hoc" reporting systems allow the users themselves to create specific, customized queries. Typically this would be via a user-friendly GUI-based system without the need for the in-depth knowledge of SQL, or database schema that a programmer would have.

Because such reporting has the potential to severely degrade the performance of a live system, it is most usual to be provided over a Data Warehouse. Ad hoc querying/reporting is a Business Intelligence subtopic, along with OLAP, Data Warehousing, Data Mining and others tools.

9. Conclusion

In this paper, we have analyzed the security threats an ad hoc network faces and presented the security objectives that need to be achieved. On one hand, the security-sensitive applications of ad hoc networks require high degree of security; on the other hand, ad ho c networks are inherently vulnerable to security attacks. Therefore, security mechanisms are indispensable for ad ho c networks. The idiosyncrasy of ad ho c networks poses both challenges and opportunities for these mechanisms.

This paper focuses on how to secure routing and how to establish a secure key management service in an ad hoc networking environment. These two issues are essential to achieving our security goals. Besides the standard security mechanisms, we take advantage of the redundancies in ad hoc network topology and use diversity coding on multiple routes to tolerate both benign and Byzantine failures. To build a highly available and highly secure key management service, we propose to use threshold cryptography to distribute trust among a set of servers. Furthermore, our key management service employs share refreshing to achieve proactive security and to adapt to changes in the network in a scalable way. Finally, by relaxing the consistency requirement on the servers, our service does not rely on synchrony assumptions. Such assumptions could lead to vulnerability. A prototype of the key management service has been implemented, which shows its feasibility. The paper represents the first step of our research to analyze the security threats, to understand the security requirements for ad hoc networks, and to identify existing techniques, as well as to propose new mechanisms to secure ad hoc networks. More work needs to be done to deploy these security mechanisms in an ad hoc network and to investigate the impact of these security mechanisms on the network performance.

10. References

[1] Carroll, Robert T. "Ad hoc hypothesis." The Skeptic's Dictionary. 22 Jun. 2008.

[2] Texas A&M University. "Einstein's Biggest Blunder? Dark Energy May Be Consistent With Cosmological Constant." ScienceDaily 28 November 2007. 22 June 2008.

[3] Ayanoglu E., Gitlin R. D. and Mazo J. E. (1993) *IEEE Transactions on Communications*, 41(11):1677–1686.

[4] *Castro M. and Liskov B. (1999) Proceedings of the 3rd USENIX Symposium on Operating System Design and Implementation (OSDI'99),* 173–186. *USENIX Association, IEEE TCOS, and ACM SIGOPS.*

[5] Desmedt Y. (1994) *European Transactions on Telecommunications,* 5(4):449–457.

[6] Desmedt Y. and Frankel Y. (1989) *Crypto'89, the 9th Annual International Cryptology Conference, Santa Barbara, CA USA, August 20–24, 1989, Proceedings, volume 435 of Lecture Notes in Computer Science, pages 307–315. Springer,* 1990.

[7] Desmedt Y. and Jajo dia S. (1997) *Technical Report ISSE TR-97-01, George Mason University*.

[8] Ephremides J. E., Wieselthier and Baker D. J. (1987) *Proceedings of the IEEE*, 75(1):56–73.

[9] Feldman P. (1987) *Proceedings of the 28th Annual Symposium on the Foundations of Computer Science*, 427–437.

[10] Fischer M. J., Lynch N. A. and Peterson M.S. (1985) *Journal of the ACM*, 32(2):374–382.

[11] Frankel Y., Gemmel P., MacKenzie P. and Yung M. (1997) *Proceedings of the 38th Symposium on Foundations of Computer Science*, 384–393.

[12] Frankel Y., Gemmell P., MacKenzie P. and Yung M. (1997) B. *S. Kaliski Jr., editor, Advances in Cryptology—Crypto'97, the 17th Annual International Cryptology Conference, Santa Bar- bara, CA USA*.

[13] Gasser M., Goldstein A., Kaufman C. and Lampson B. (1989) *Proceedings of the 12th National Computer Security Conference*, 305–319.

[14] Gennaro R., Jarecki S., Krawczyk H. and Rabin T. (1996) N. Koblitz, editor, Advances in Cryptology—Crypto'96, the 16th Annual International Cryptology Conference, Santa Barbara, CA USA, August 18–22, 1996.

[15] Gennaro R., Jarecki S., Krawczyk H. and Rabin T. (1996) U. M. Maurer, editor, Advances in Cryptology—Eurocrypt'96, International Conference on the Theory and Application of Cryptographic Techniques, Saragossa, Spain, May 12–16, 1996.

[16] Gong L. (1993) *IEEE Journal on Selected Areas in Communications*, 11(5):657–662.

[17] Haas Z.J. and Liang B. (1999) *IEEE/ACM Transactions on Networking*.

[18] Haas Z.J. and Perlman M. (1998) *In SIGCOMM'98*.

[19] Hassan W., Stark E. and Hershey J. E. (1993) *Transactions on Communications*, 41(7):1125–1131.

[20] Hauser R., Przygienda T. and Tsudik G. (1999) *Computer Networks*, 31(8):885–894.

[21] Herzberg M., Jakobsson S., Jarecki H., Krawczyk and Yung M. (1997) *Proceedings of the 4th Annual Conference on Computer Communications Security*, 100–110.

[22] Herzberg S., Jarecki H., Krawczyk and Yung M. (1995) *D. Coppersmith, editor, Advances in Cryptology—Crypto'95, the 15th Annual In- ternational Cryptology Conference, Santa Barbara, CA USA*.

[23] Ioannidis J., Duchamp D. and Gerald J. M. (1991) *ACM SIGCOMM Computer Communication Review (SIGCOMM'91)*, 21(4):235–245.

[24] Jacobs S. and Corson M. S. (1999) *MANET authentication architecture. Internet Draft (draft-jacobs-imep- auth-arch-01.txt)*.

[25] Jacquet P., Muhlethaler P. and Qayyum A. (1998) *IETF MANET, Internet Draft*.

[26] Jarecki S. (1995) *Proactive secret sharing and public key cryptosystems. Master's thesis, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, MA USA*.

[27] Johnson D. B. and Maltz D. A. (1996) *Mobile Computing*.

[28] Kaufman (1993) *DASS: Distributed authentication security service. Request for Comments* 1507.

[29] Kumar (1993) *SIGSAC Reviews*, 11(2):18–25.

[30] Malkhi and Reiter M. (1998) *Distributed Computing*, 11(4):203–213.

[31] Malkhi and Reiter M. (1998) *Proceedings of the 17th Symposium on Reliable Distributed Systems*, 51–58.

[32] Murphy S. and Garcia-Luna-Aceves J. J. (1996) *MONET*, 1(2):183–197.

[33] Ostrovsky R. and Yung M. (1991)*Proceedings of the 10th Annual Symposium on Principles of Distributed Computing (PODC'91),* 51–59.

[34] Park V. D. and Corson M. S. (1997) *In IEEE INFOCOMM'97, Kobe, Japan*.